UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,814	03/07/2002	Yoshihito Taninaka	3620-P02831US0	7974

110 7590 06/01/2005

DANN, DORFMAN, HERRELL & SKILLMAN
1601 MARKET STREET
SUITE 2400
PHILADELPHIA, PA 19103-2307

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,814	TANINAKA ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 March 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☒ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 56, 57 (page 21, lines 2-3). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The

abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

3. The disclosure is objected to because of the following informalities: "countermeasure been taken" (page 3, line23), "that have not be dealt" (page 4, lines 6-7). Appropriate correction is required.

4. The disclosure is objected to because of the following informalities: "CPU" (page 14, line 18), "RAM" (page 14, line 20). While well known in the art, these terms have not been defined.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fox et al. (US Patent Number: 6,535,227), and further in view of Alves-Foss et al. (NPL Document: Assessing Computer Security Vulnerability).

Regarding claim 1, Fox et al. teach a method for offering security level comprising the steps of: (a) specifying, based on configuration information on a specific equipment, a vulnerability of said equipment, and associating information of the vulnerability with said equipment, said information of the vulnerability including a threat level value of the vulnerability (column 7, lines 45-60); (b) computing a security level value of the vulnerability of the specific equipment (column 7, lines 45-60); and (c) outputting security level information based on the security level value obtained in said step (b) (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25). Fox et al. do not disclose expressly threat level value of the vulnerability based on the type of this equipment, the threat level value of the vulnerability for which no modification has been taken regarding this equipment, and the number of days while the vulnerability has been left without any modification taken for the vulnerability. Fox et al. combine multiple types of data, from multiple sources, with other contextual information to from an integrated view of a networked system's security posture (column 11, lines 1-10). However, Alves-

Foss et al. teach measuring a System Vulnerability Index based on system characteristics, potentially neglectful acts, and potentially malevolent acts (pages 4-12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compute a security level value based on the type of this equipment, the threat level value of the vulnerability for which no modification has been taken regarding this equipment, and the number of days while the vulnerability has been left without any modification taken for the vulnerability. One of ordinary skill in the art would have been motivated to perform such a modification to because it was well known in the art at the time the invention was made to combine multiple types of data to assess the security of a system and provide a gauge for appraising system vulnerabilities (Alves-Foss et al., pages 3-6).

Regarding claim 2, the combination of Fox et al. and Alves-Foss et al. teach the limitations as set forth under claim 1 above. Furthermore, Alves-Foss et al. teach (d) computing a security level value of said equipment by comparing the security level values of vulnerabilities when there are a plurality of vulnerabilities associated with said equipment, which have not been modified, and setting a security level value with the highest threat level value among the security level values of said vulnerabilities as the security level value of said equipment, and wherein said step (c) outputs the security level information based on the security value of said equipment obtained in step (d) (pages 4-12). The reasoning for combining is the same as that for claim 1 above.

Regarding claim 3, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 2 above. Furthermore, Fox et al. teach (e)

computing the security level value of a network when a plurality of equipments are connected to the network, by comparing security level values of the equipments, and setting a security level value with the highest threat level value among the security level values of said equipments as the security level value of said network (column 7, lines 45-67, column 8, lines 44-67), and wherein said step (c) outputs security level information based on the security value of said network (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25).

Regarding claim 4, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 1 above. Furthermore, Fox et al. teach wherein said step (c) outputs security information based on both security level value obtained in the step (b) and basic security information computed based on a basic configuration, etc. of the equipment or the network (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25).

Regarding claim 5, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 1 above. Furthermore, Alves-Foss et al. teach wherein said step (c) comprises a step of expressing said security level value in comparison with a security level reference value of a relevant system or the network to which said system is connected (pages 3-9). The reasoning for combining is the same as that for claim 1 above.

Regarding claim 6, Fox et al. teach a configuration information storing unit for storing configuration information on the computer system to be monitored (column 9, lines 5-15); a vulnerability information storing unit for storing various types of updated

vulnerability information including at least a threat level value of the vulnerability (column 15, lines 25-32); a vulnerability information offering unit to extract vulnerability information to be applied to said computer system from said vulnerability information storing unit based on said configuration information, and to associate the vulnerability information with this computer system (column 7, lines 45-60); a security level computing unit for computing, regarding a specific equipment, a security level regarding the vulnerability of said equipment (column 7, lines 45-60); and a security level information generating unit for generating and output security level information based on the security level value obtained in said computing unit (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25). Fox et al. do not disclose expressly a vulnerability modification information storing unit for storing the information on whether or not a system manager has applied modification work based on this vulnerability information. However, Examiner takes Official Notice that storing information regarding the actions taken on a particular task was conventional and well known. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store a modification log related to actions taken regarding vulnerabilities found since Examiner takes Official Notice that it was conventional and well known. Fox et al. do not disclose expressly computing a security level regarding the vulnerability of said equipment from a type of this equipment, the threat level value of the vulnerability that has not been modified with regarding this equipment, and the number or days while the vulnerability has been left without any modification taken. Fox et al. combine multiple types of data, from multiple sources, with other contextual information to from an

integrated view of a networked system's security posture (column 11, lines 1-10). However, Alves-Foss et al. teach measuring a System Vulnerability Index based on system characteristics, potentially neglectful acts, and potentially malevolent acts (pages 4-12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compute a security level value based on the type of this equipment, the threat level value of the vulnerability for which no modification has been taken regarding this equipment, and the number of days while the vulnerability has been left without any modification taken for the vulnerability. One of ordinary skill in the art would have been motivated to perform such a modification to because it was well known in the art at the time the invention was made to combine multiple types of data to assess the security of a system and provide a gauge for appraising system vulnerabilities (Alves-Foss et al., pages 3-6).

Regarding claim 7, the combination of Fox et al. and Alves-Foss et al. teach the limitations as set forth under claim 6 above. Furthermore, Alves-Foss et al. teach a security level value comparing unit to compute a security level value of said equipment by comparing security level values of vulnerabilities when there are a plurality of vulnerabilities associated with said equipment, which have not been modified, and setting a security level value with the highest threat level among the security level values of said vulnerabilities as the security level value of said equipment, and wherein said security level information generating unit generates security level information based on said security level value of said equipment computed by the security level

value comparing unit (pages 4-12). The reasoning for combining is the same as that for claim 6 above.

Regarding claim 8, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 7 above. Furthermore, Fox et al. teach wherein said security-level value comparing unit computes a security value of a network by comparing security level values of equipments when a plurality of equipments are connected to said network, and setting a security level value with the highest level of threat among the security level values of said equipments as the security value level of said network (column 7, lines 45-67, column 8, lines 44-67); and said security level information generating unit outputs security level information based on the security level value of said network computed by the security level value comparing unit (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25).

Regarding claim 9, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 6 above. Furthermore, Fox et al. teach wherein said security level information generating unit outputs security information based on both security value obtained in said security level computing unit and basic security information computed based on a basic configuration, etc. of an equipment or a network (column 7, lines 45-60, column 8, lines 64-67, column 9, lines 1-25).

Regarding claim 10, the combination of Fox et al. and Alves-Foss et al. teaches the limitations as set forth under claim 6 above. Furthermore, Alves-Foss et al. teach wherein said security level information generating unit expresses said security level value in comparison with a security reference value of a relevant system or the network

to which this system is connected (pages 3-9). The reasoning for combining is the same as that for claim 6 above.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100